Journal of King Saud University – Computer and Information Sciences (2017) **29**, 269–280

King Saud University

Journal of King Saud University – Computer and Information Sciences

www.ksu.edu.sa
www.sciencedirect.com

F3TM: Flooding Factor based Trust Management Framework for secure data transmission in MANETs

Malik N. Ahmed *, **Abdul Hanan Abdullah, Hassan Chizari, Omprakash Kaiwartya**

Faculty of Computing, Universiti Teknologi Malaysia, Johor, Malaysia

Received 17 November 2015; revised 30 March 2016; accepted 30 March 2016
Available online 20 April 2016

KEYWORDS

Route Discovery;
True flooding;
Route Request Route Replay;
Routing efficiency;
Enhanced Multi-Swarm Optimization

Abstract Due to the absence of infrastructure support, secure data dissemination is a challenging task in scalable mobile ad hoc networks (MANETs) environment. In most of the traditional routing techniques for MANETs, either security has not been taken into account or only one aspect of security concern has been addressed without optimizing the routing performance. This paper proposes Flooding Factor based Framework for Trust Management (F3TM) in MANETs. True flooding approach is utilized to identify attacker nodes based on the calculation of trust value. Route Discovery Algorithm is developed to discover an efficient and secure path for data forwarding using Experimental Grey Wolf algorithm for validating network nodes. Enhanced Multi-Swarm Optimization is used to optimize the identified delivery path. Simulations are carried out in ns2 to assess and compare the performance of F3TM with the state-of-the-art frameworks: CORMAN and PRIME considering the metrics including delay, packet delivery ration, overhead and throughput. The performance assessment attests the reliable security of F3TM compared to the state-of-the-art frameworks.

1. Introduction

Mobile ad hoc networks (MANETs) have an enormous number of networks and hops, without any closed infrastructure and protected secure data transmission. In this situation, whenever a node communicates and shares data with other nodes on the network, various problems will occur such as the route path, attacker interruption (McNerney and Zhang, 2012) and data delivery problems. To avoid these problems, it is possible to use the following approaches including the Route Discovery Algorithm, the True flooding algorithm (TFA), the Route Request, Route Replay method, and Routing efficiency (Lafta and Al-Salih, 2014), along with the Network Overload Method and the Enhanced Multi-Swarm Optimization method. The results of the above stated problems show that each mobile ad hoc network can detect malicious nodes, and start communicating through the secure path using this study's proposed system.

This work has dealt with past interaction history-based recognition and avoidance of malicious nodes and Denial-of-Service attacks on the network layer, namely Grayhole,

* Corresponding author.

Peer review under responsibility of King Saud University.

ELSEVIER Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.jksuci.2016.03.004

Blackhole or Wormhole (Jaiswal and Sharma, 2012; Gorlatova et al., 2006) attacks through the use of this study's proposed scheme, specifically a minimized secure True flooding trust value scheme (MSTFTV) (Vadivel and Narasimhan, 2014). This scheme always provides a flooding factor, and indicates the presence of the attacker node and its attack.

In this regard, both the sender-based MSTFTV scheme and the receiver-based MSTFTV scheme are also used to discover the flooding factor. Flooding factor results show that the proposed scheme detects malicious nodes and improves routing paths (Assis and Giozza, 2010). A list of ad hoc protocols is needed to control how nodes decide the way to route packets, with respect to the source node and destination nodes. All those types of protocols are classified based on a number of constrains, including expensive infrastructure, the distribution of information, network functions, central entities, Route Request, and number of nodes. All those constraints are periodically used in any type of flooding attack on the Reactive Routing.

The rest of the paper is organized as follows. Section 2 reviews related works on secure data transmission frameworks. Section 3 presents Key Assignment Algorithm, then the proposed optimization algorithm is given in Section 4. True flooding algorithm, itinerant algorithm, and past interaction history are presented in Sections 5,6, and 8 respectively. The result and performance analysis is explained in Section 4. Then the work is concluded in Section 9

2. Related works

Chang et al. (2008) have proposed a model to analyze the trust value for a sender sending packets to several receivers, through a multicast session. Since members of a multicast group change frequently, the issue of supporting secure authentication and authorization in multicast MANET becomes more critical than the network providing a fixed central authentication (CA) server. To overcome this effort, this study introduces the Head_CV consideration, and this Head_CV gives the CA authority to individual nodes for the ignored time period. Within this time period, the normal node will determine whether the neighbor node is malicious or not (Chang et al., 2008).

Al Mazrouei and Narayanaswami (2011) have proposed a mechanism to detect and remove Blackhole and Grayhole attacks (Al Mazrouei and Narayanaswami, 2011). Their proposed solution tackles these attacks by maintaining an Extended Data Routing Information (EDRI) Table at each node, in addition to the Routing Table of the AODV routing protocol. To overcome this effort, this study introduces the past interaction history-based pattern for storing new transactions for every node over the network.

Wang et al. has proposed the Cooperative Opportunistic Routing in Mobile Ad Hoc Networks (CORMAN) (Wang et al., 2012). It was a remedy for accepting as a challenge behind the opportunistic data transfer of mobile ad hoc networks. The solution is to test CORMAN and to compare it to AODV, and to observe significant performance improvement in varying mobile settings. CORMAN uses the Nakagami fading model in ns-2, and compares it to the well-understood AODV in an array of mobile network scenarios. The performance improvement of CORMAN they observed is substantial. Contributions through their solution are highlighted as a means of finding the path selection aspect through a correct manner. Consequently they use the lightweight proactive source routing protocol, so that each node has complete knowledge of how to route data to all other nodes in the network, at any time.

McNerney and Zhang (2012) demonstrated through the use of a simulation study that the single-path adaptation approach to MANET QoS provisioning (McNerney and Zhang, 2012; Long et al., 2013) is no longer sufficient in adversarial environments. It identifies the conditions in which an additional measure, for instance an adaptive multi-path routing extension, may be necessary for maintaining service quality. The study uses the INSIGNIA signaling system as a facilitator of the single-path adaptation approach, and evaluates its effectiveness in the presence of Blackhole and Grayhole data forwarding attacks and a denial of a QoS request attack on QoS signaling (McNerney and Zhang, 2012; Rmayti et al., 2014a). Results are evaluated through the use of a service quality metric defined in this paper. To overcome this effort, this study introduces the Itinerant algorithm, and also it finds that the efficient sender-based Minimized secures the True flooding trust value scheme, and that the Receiver-based Minimized secures the True flooding trust value scheme.

Rmayti et al. (2014b) have proposed a novel approach to watchdog, based on two Bayesian filters, particularly those of Bernoulli and Multinomial (Rmayti et al., 2014b). This study uses these two models in a complementary manner, in order to successfully detect the packet dropping attacks in mobile ad hoc networks. Based on the simulation results, the study's proposed filters have proven that these attacks can be detected with a high rate of accuracy. To overcome this effort, the Enhanced Multi-Swam Optimization Algorithm has been introduced as a means to prevent the mobility node Location, pattern route path, time taken for send data packet, and the Time taken for receive data packet. This study overcame these issues through the ID assignment to the node, namely the Node IdDS.

The routing method of Perkins et al. (2006) allows for a collection of nodes exchange data through various paths, with respect to the multi-hop path of interconnection (Perkins and Bhagwat, 1994). Within networks, each station of nodes store their Routing Tables, which are useful for transmitting packets between the stations, due to the performing path between those stations. Such a Routing Table contains all the numbers of hops, and also the available destinations. Each route table entry is tagged with a sequence number, which originates at the destination station. Each station periodically transmits updates, and then transmits those updates immediately when significant new information is available. Also it makes no assumptions about the phase relationship of the update periods between the mobile hosts. These packets indicate which stations are accessible from each station, and the number of hops necessary to reach these accessible stations, as is often achieved through distance-vector routing algorithms. The DSDV protocol requires each mobile station to advertise its own Routing Table to each of its current neighbors. In this way, a mobile computer may exchange data with any other mobile computer in the group, even if the target of the data is not within the range of direct communication.

Garcia-Luna-Aceves et al. proposed the PRIME framework based on interest-defined mesh enclaves, which is the

proposed framework for integrated routing in MANETs (Garcia-Luna-Aceves and Menchaca-Mendez, 2011). When compared with the traditional unicast and multicast routing schemes for MANETs, like AODV, OLSR and ODMRP, the benefit of PRIME is that it gains with the effort of similar or better data delivery and end-to-end delays. In addition to that approach, this is used for routing, and the distinction between on-demand and proactive signaling for routing is eliminated. Interest-driven signaling is used instead. A comparison of the performance of PRIME with some relevant multicast and unicast routing protocols for MANETs is described based on the routing protocols, supporting unicast traffic, multicast traffic, and a combination of both. The main focus of PRIME is minimum-hop routing, which compares PRIME to ODMRP and PUMA, in order to determine the effectiveness of PRIME as a multicast routing protocol. In the case of unicast traffic, they compare PRIME against OLSR and AODV, and vary the number of concurrent unicast flows and node density.

The scheme proposed by Vadivel and Narasimhan (2014) has two algorithms, namely the sender-phase algorithm and the receiver-phase algorithm. The sender-phase algorithm of the proposed work aids a node in selecting a subset of neighbors to forward the flooding message (Vadivel and Narasimhan, 2014). The sender-phase algorithm selects forwarding nodes with the highest contribution to flooding message dissemination. To overcome this effort, this study introduces a new TFA to find a MSTFTV scheme based on the flooding factor. Here the Node has an ID-based digital signature key, so it is very challenging to calculate some performance metrics like trust value (Wei et al., 2014), and time to delay and attacks, but it is possible to overcome all these issues.

Fig. 1 shows the overall Architecture of F3TM, which consists of five process phases including the IdDS-Key Assignment Algorithm, the TFA for finding trust value can be briefly declared, and from this the attacker can be found, the Route Discovery Algorithm can discover the efficient secure path, the Route Request Route Replay method can be used for the packet delivery ratio, the New Experimental Grey Wolf algorithm can be used to validate nodes, and the Enhanced Multi-Swarm Optimization method can be used for optimizing the attacker node.

3. Key Assignment Algorithm (KAA)

The Key Assignment Algorithm is an Identification-based Digital signature, encouraged by the Head_CA to send ID-based Digital signature keys to many mobile nodes, in order to secure the nodes within the boundary level for awareness of malicious node attacks. The individual key has been randomly driven through from the neighbor node (Jain and Raisinghani, 2014) to the destination node, in the form of a packet. The key generation algorithm evolves an existing key management scheme to a new secure node Key management scheme.

Fig. 2 shows the key assignment process of the node initialization presence of the digital signature. The following description gives the initialization of nodes, with bandwidth and latency calculated through using the Digital signature.

3.1. IdDS-Key Assignment Algorithm (KAA)

The IdDS-Key Assignment Algorithm describes, finds and assigns keys to individual nodes within the network, and describes node properties that correspond to bandwidth, node life time, and node latency. It also provides a security mechanism (Al Mazrouei and Narayanaswami, 2011; Lacharité et al., 2008) to the individual nodes, instead of giving a digital signature to individual nodes through cluster agents in the network groups. It gives a secure key assignment to each and every node based IdDS-Key Assignment Algorithm. KAA is described through the algorithm proposed below.

Let N be the total No. of Node, $\mathbb{MN}$ (MANET Network), which consists of:

$$\mathbb{MN} = \{N1, N2, N3, N4, .., Nl\}\ \forall N\ \varepsilon \mathbb{MN} \tag{1}$$

We can calculate α, β, and δ for individual nodes from the bandwidth of hop, node lifetime (TTL) and node latency, where ω is assigned to the individual mobile node, α to the node bandwidth, β to the node life time, and δ to the node latency.

Find the bandwidth of the individual node with the cluster agent through the following formulae.

First and foremost, Node latency is calculated through the following three fields,

$$\text{Latency}(\delta) = \langle \text{snd initial signal pkts} | \text{rcvd valid signal pkts} | \text{time consume} \rangle$$

$$\text{Bandwidth}(\alpha) = \frac{\text{Network size}(N) = \sum_{n=1}^{l}(x)}{\text{Latency}(\delta)} \tag{2}$$

To discover the valid node V of the individual nodes in group ($\mathbb{MN}$):

$$V = \sum_{N=1}^{l} \mathbb{MN} \log_2 \frac{(\text{Bandwidth} | \text{life time})}{\text{Latency}} \tag{3}$$

V is equal to the total number of nodes available in the particular group.

After validating all nodes in the particular group ($\mathbb{MN}$), the digital signature key is sent through the HCA node and thus, the node has a secure key with a Key Assignment Algorithm (KAA):

$$\mathbb{MN} = \{N1_{k_1}, N2_{k_2}, N3_{k_3}, N4_{k_4}, \ldots, Nl_{k_m}\} \tag{4}$$

The digital signature key is assigned through the following description:

ω is the digital signature key assignment:

$$\omega = \{(V|N1_{k_1}), (V|N2_{k_2}), (V|N3_{k_3}), (V|N4_{k_4}), \ldots, (V|Nl_{k_m})\}\ \forall V, N \varepsilon \mathbb{MN} \tag{5}$$

After assigning the secure key to the individual node, each node has the ability to connect the HCA node (Head Cluster Agent) and clustering groups, based on the related digital signature key, and also maintains the signal strength of each node with the help of hop mobility, and high secure acquisition prominence.

Prominently the entire Key Assignment Algorithm (KAA) gives Node Shaping Optimization, Security Performance (Al Mazrouei and Narayanaswami, 2011; Lacharité et al., 2008), Improved Latency, and/or also usable bandwidth for some

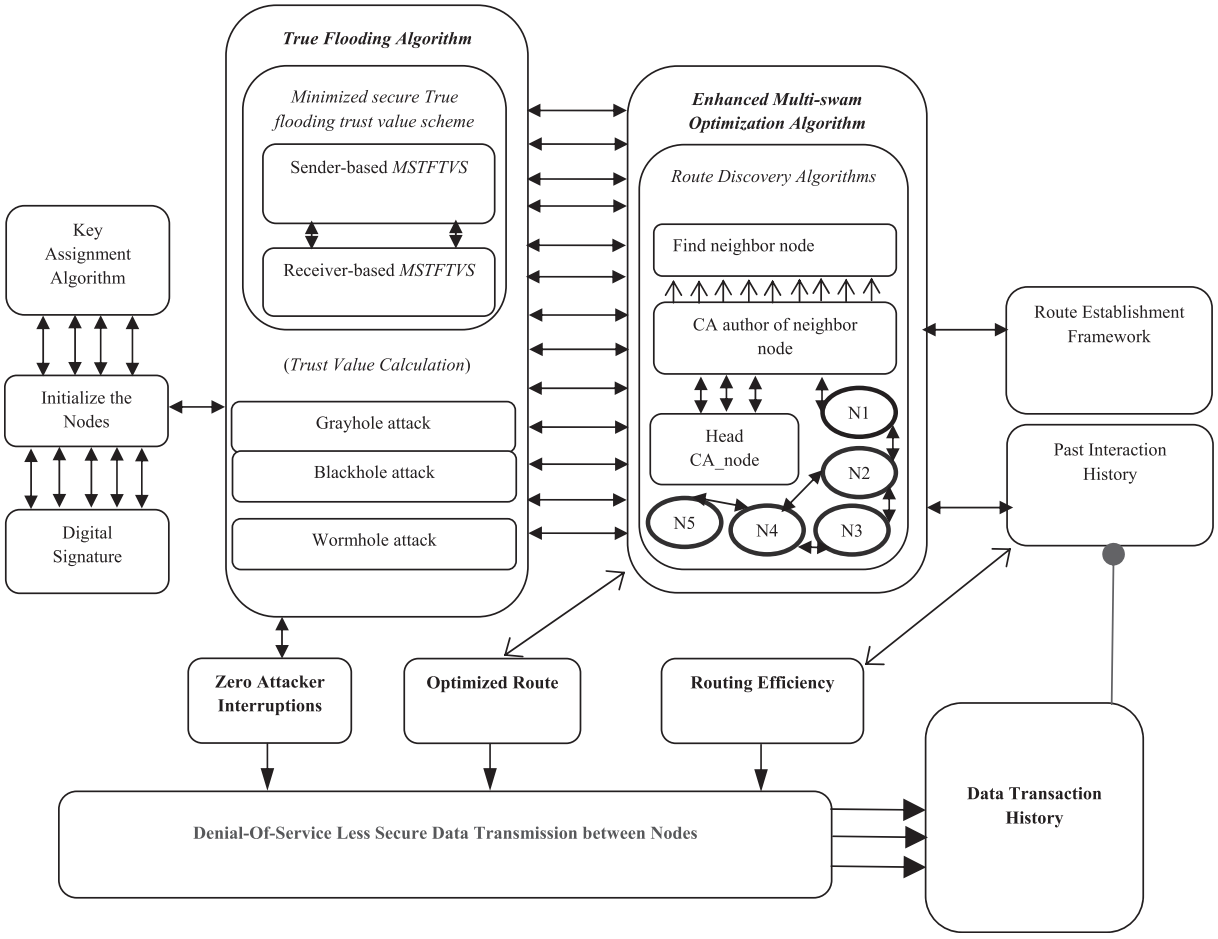

Figure 1 F3TM architecture.

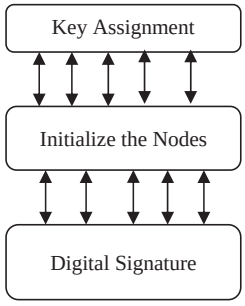

Figure 2 IdDS-Key Assignment Algorithm.

kinds of nodes, which gives some kinds of involuntary traffic shaping effects.

3.2. Algorithm for the Key Assignment

For assigning keys to the individual nodes in the network, we can follow the below description for allocating secure keys with identification-based digital signatures.

The Key Assignment Algorithm is used for allocating the key, by calculating the bandwidth and latency of the node. It will direct to finding the node bandwidth and assigning a digital signature. Bandwidth is useful for finding the trust value calculation and digital signature, bringing it into being the node security at the entire transmission. To find the shortest path based on the node count, first we derive the best routing path, with consideration of both the trust values and the number of network node counts. It may be the start node of the destination node with respect to the gate way. The hop count is likened to the number of iterations to the network nodes. This may be constructed based on the TFA. We use Route Discovery Algorithms to calculate the best routing path, and we need to convert the Flooding Factor to the trust value. The trust value calculation is based on the following equation, which gives the trust value to the individual node, and is stored back to past interaction history:

$$\text{Trust value(Start\_Node)} = \text{Flooding Factor(Start\_Node)}$$
$$\text{Trust value(Dest\_Node)} = \text{Flooding Factor(Dest\_Node)}$$

The sum of the trust values in the path is:

$$\text{Trust values}(\text{Start}_{\text{Node}}|\text{Dest}_{\text{Node}}) = \sum_{x=1}^{\text{MN}-1}\sum_{y=1}^{\text{MN}-1}\{x - \text{FF(SN)}\} + \{y - \text{FF(DN)}\} \quad (6)$$

where MN is the MANET network nodes which consists of the group of the Start node (SN) and the Destination node (DN), x is the total number of the network size with respect to the source region of MN, and y is the total number of the network

size with respect to the destination region of MN. The trust values of each node can be stored in the trust values table, which provides additional security protection to open environments with a combination of software and hardware. Since the trust values in each node are the key facilities for detecting malicious nodes, they provide effective protection to secure routing and avoid malicious attacks by enemies in combat zones.

4. Proposed optimization algorithm

4.1. New Experimental Grey Wolf and Swam Optimizer-(NEGSO)

The new experimental was the work stated by Grey Wolf Optimizer (GWO). The GWO algorithm simulates the leadership hierarchy (Clustering Head), and the chasing mechanism (Node Finding Mechanism) of grey (old) wolves (womanizers) in nature. Based on the New Experimental Grey Wolf and Swam Optimizer-(NEGSO) procedure, we find nodes with key values and also checking the node details like node id, node bandwidth, and node life time through the use of the NEGSO's Key Assignment Algorithm. Four types of old womanizers, including alpha (α), beta (β), delta (δ) and omega (ω), are active in simulating the leadership hierarchy. In addition, four main steps are required to find an attacker node within the group of nodes:

1. Chasing the nodes.
2. Searching for target nodes.
3. Inclosing the target nodes.
4. Attacking the target nodes.

These steps are very much useful in searching an individual node, and also in finding an attacker node with the help of trust value (Chang et al., 2008; Yang et al., 2014) calculation. Here we have to use the flooding factor (Vadivel and Narasimhan, 2014) to find trust value (Chang et al., 2008) implemented between nodes, as the minimum flooding factor for which each node is flooded. This flooding factor permits the sender-based MSTFTV scheme and the receiver-based MSTFTV scheme, using the MSTFTV scheme. As it gives, all trust values (Chang et al., 2008) were calculated and compared to the past interaction history (PIH). Here the PIH is a collection of all previous tasks and checks the previous flooding history (Vadivel and Narasimhan, 2014), through which the highest flooding factor rapidly finds a secure path between them.

4.2. Enhanced Multi-Swam Optimization Algorithm (EM-SOA)

The Enhanced Multi-Swam Optimization Algorithm reduces the gatherings of malicious nodes, by using the optimization attacker node within the network.

1. Chasing the nodes

Individual nodes need to be found, and keys need to be assigned to each node, using the IdDS-Key Assignment Algorithms with digital signatures.

2. Searching for target nodes

Search and find the node with properties similar to the CA. This also proves the GWO algorithm. If we originate the node within the CA boundary, the presence of the key allocation algorithm and all digital signatures given to the individual nodes, the target node will be found based on the route (path) selection. With the help of the path finding algorithm, the node's key, the lifetime (time to live) and the bandwidth of the node, we can calculate the target individual node. After finding this target node, the data will be shared between the trusted nodes.

3. Surrounding target nodes

With the help of the trusted target nodes (Qureshi et al., 2010) the nearby nodes are observed through the following ways. Firstly, based on the decreased trust value, we have to give a CA authority to each and every node in the network. Each node has a CA authority to determine if the nearest node is an attacker or not. Then all CA nodes send their own ROUTE REQUEST key packets to the nearest neighbor node, and obtain ROUTE REPLAY key packets from valid users. The ROUTE REPLAY key packets are checked and compared with past interaction histories. Checking and comparing results show that the node is ready to communicate with the Head CA node for secure data sharing. In this manner, the Route finding algorithm Enhanced has simulated annealing and the Enhanced TABU search (Dahiya and Johari, 2014) is present when finding neighboring (Jain and Raisinghani, 2014) target nodes.

EM-SOA is an algorithm which reduces the gatherings of malicious nodes, using the optimization attacker node within the network. It is wide-ranging, and there is no structure for the network to detect difficult nodes, which involves data sharing within the network.

Because each and every node travels from place to place, these nodes are called itinerant nodes. This time the node properties change according to the following criteria: location, pattern route path, time to the send packet, and time to the received packet.

The itinerant algorithm is a compromise of four related issues. When it occurs on the mobility of nodes, we use the following steps with regard to the itinerant algorithm:

1. ID assignment to the node.
2. Node IdDS-Key Assignment Algorithm.

Fig. 3 shows the Enhanced Multi-Swam Optimization, which is used to optimize the attacker node. Here the Route Discovery Algorithms are used to discover the efficient secure path of nodes; and CA authentication used for finding the actual neighbor node, as well as maintaining the Head CA_Node. The Head CA_Node is used for control over the nearby neighbor node (Jain and Raisinghani, 2014). Finally, the node validation must be performed through the New Excremental Grey Wolf algorithm.

5. True flooding algorithm

The True flooding algorithm allows nodes to have an independent digital signature key form Head_CA and delivers the

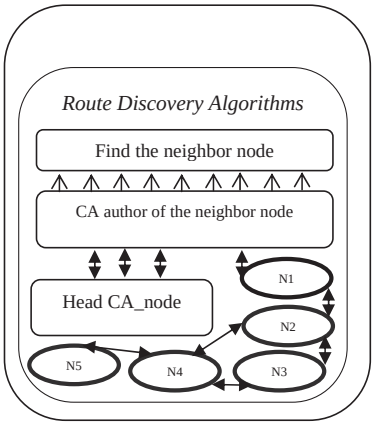

Figure 3 Diagram of the Enhanced Multi-Swam Optimization Algorithm.

highest probability that a node and link (route) fails, due to the behavior of the attacker node and normal node. It initially starts with the node that does not have any key assignment from the HEAD_CA node. In this case, the start node or initial node is identified based on the HEAD_CA packet token delivery to the neighbor node (Jain and Raisinghani, 2014). The valid node is consumed as a communicating node, without any interruption for the packet sent over the network.

After finding the initial node, the key will be assigned using the IdDS-Key Assignment Algorithm, and the node which has the IdDS key is named the secure node of the network. The flooding factor is calculated through the use of the TFA, as derived below. From that we require the key allotted Start node, the Destination node, the Neighbor node, and the trust value to the individual node, in order to find the Flooding Factor. From the Flooding Factor, finally we find the minimum route of nodes. This also gives the MSTFTV scheme for finding the trust value for finding attacks (Yang et al., 2014). Here we find and detect the individual node properties, regardless of whether the node is malicious or not.

Fig. 4 describes the TFA used for calculating the trust value for the purpose of finding attackers. Here the MSTFTV scheme is used on both the sender and receiver sides. The trust value (Chang et al., 2008) calculation will be appropriate even

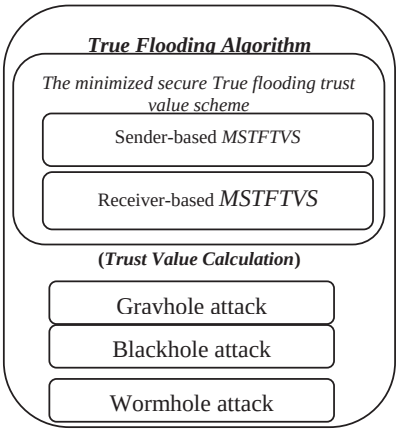

Figure 4 Diagram of the True flooding algorithm.

in the case of Grayhole, Blackhole (Bindra et al., 2012), and Wormhole attacks (Gorlatova et al., 2006). Finally, node attackers must be discovered through the use of the TFA.

Generally, the TFA has four main criteria which can be used to find the three different attacks, including the Blackhole attack, the Wormhole attack, and the Grayhole attack. The TFA is very much useful for the invention of the Blackhole attack for the following descriptions, including node selection, finding the packet loss, finding the trace route, and finding the attacker route path, all of which are helpful to traffic occurrence due to an attacker. All those attackers are refined by the TFA, to accomplish the Blackhole attacks. Similarly, the TFA finds the Wormhole attack, and the Grayhole attack by the attacker route path is derived from the traffic occurrence on the route. If the traffic is positive, the malicious node occurrence is also positive. This type of attack is called a Wormhole attack, which is reduced through the following consumption. Firstly, tunneling allows a network user to access or provide a network service that the underlying network does not support or directly provide. The tunneling protocol is used to allow a foreign protocol to run over a network that does not support that particular protocol. In addition to that, the tunneling protocol works using the data portion of a packet to carry the packets that actually provide the service. Secondly, the Packet Location disclosure (Manikandan et al., 2011) attack is a part of the information disclosure attack. The malicious node leaks information regarding the location or structure of the network, and uses the information to implement further attacks. It gathers the node location information, such as a route map, and knows which nodes are situated on the target route. Traffic analysis is one of the unsolved security attacks used against MANETs. Thirdly, the patterns, specifically the traffic pattern and the actual pattern, are recognized by the path route algorithm used for pattern loss. In terms of the Wormhole attack, the derivation of the Grayhole attacks is used firstly for reducing packet delay, secondly for gaining energy consumption, and thirdly for enhancing the packet delivery ratio. As a final point, these processes are used to calculate packet delivery ratio and to reduce packet loss.

6. Itinerant algorithm

Based on node properties, if we want to obtain the correct position of the normal node, we must obtain at least the id assignment of the node independent measurements of the location, the pattern route path, the time to send the packet, and the time to receive the packet. All are needed for the location or position of the valid node, which is going to be communicated with each other's node, in the presence of the Head CA (Cluster Agent). After finding the itinerant associated node, it is possible to obtain zero values to each other's. Finally, the node is ready for the communication of data sharing.

Now we use the Enhanced Multi-swam optimization algorithm for deriving the node optimization. The EM-SOA consists of the following steps undertaken to find the valid optimized route between nodes.

6.1. Route Discovery Algorithms

Consists of nodes with

- node id,
- digital signature key, and
- derived itinerant less node.

Through this, the route of the shortest path can be found, based on finding which contains

Step 1.1: Head CA.
Step 1.2: Giving CA authority to the normal node.
Step 1.3: Determining if the neighbor node is attacker or not.

- Head_CA

A node which has the highest priority of trust value from the MSTFTV scheme, and that particular node acts like the head (CA) node.

- CA authority to the normal node

A node which has the selected priority of the trust value from the MSTFTV scheme (Vadivel and Narasimhan, 2014), that temporarily acts as the CA node with an ignored time period. Within this time period, the temporary node will send packets nearby for the node to check the exactness or validity of the node without any intruder available in the mobile network, and finally within this selectable time period the nearby unwanted nodes are detected. The result of the CA authority is the normal node Route Establishment Framework, which is observed and stored in the past interaction history (PIH).

6.2. Find the neighbor node

The Route Request is sent over the network to the entire individual node, to find a nearby node which has zero attackers and thus, sent back Route Reply. Also there is a need to establish a sender-based request, as well as a receiver-based reply, without the detection of any break to the valid node, until the optimized well-known route is found.

Once the path has been detected, the temporary CA node, which has ignored the time period to live, will become the normal node. This means that within the ignored time period the trustworthy full route path will be found. Simultaneously, interaction histories have been recorded using a past interaction history.

7. Past interaction history

The past transaction history contains a node identification number, a gateway to the interface node, and the metric value for the current communication. If the packet sends over the network from two different nodes, the history of source routing, Hop-by-hop routing, and the routing metric are stored in the Past Transaction History. If any routing path (Lafta and Al-Salih, 2014; Dahiya and Johari, 2014) exists while the packet is sending over nodes, the packet was not sent through that route due to two reasons, firstly because the route is already patterned, and secondly because the route has some malicious attacker. This also allows for the Delay of Intruder, Control Overhead, Packet Delivery Ratio, Energy Consumption, Queue delay and Agent Trace of the overall networks.

The analyzed values are modeled based on the following formulae, which are used to find the correct route path of any nodes. In addition to this, the attackers are making findings based on the trust values.

$$\text{Number of iterations on the same path} = \text{Number of nodes presented in the MN} * \text{cost metrics} \tag{7}$$

$$\text{Number of routes on the gateway} = \frac{\text{Number of gateway between the two nodes}}{\text{Current number of nodes to gateway interfaces}} \tag{8}$$

Eqs. (7) and (8) offer a general past interaction history, directed to find the number of nodes which are presented in the form of an attacker. The analyzed values of the past interaction history, as constructed in Table 3, is useful for finding and combining the number of iterations and number of routes in the concerned network nodes. This is used to store the previous history of the processing scheme of F3TM.

8. Performance analysis

Within the experimental analysis, the performance of network nodes is analyzed using the proposed Flooding Factor based Trust Management Framework (Guo et al., 2011).

The proposed methodology is implemented through the use of NS-2. This is a popular and well-known network simulator tool. This tool is used in the areas of MANET, wireless sensor network and others. In this work, the network consists of 100 mobile nodes and attacker nodes. The simulation model of the network is presented in Fig. 5.

8.1. Simulation parameters

Simulation parameters are used while implementing the proposed technique, which is summarized below in Table 1. These parameters are used to construct the network. The AODV protocol (Bindra et al., 2012; Gorlatova et al., 2006) is taken as an existing work, and is compared and applied to various techniques such as PRIME and CORMAN, as well as this study's proposed system F3TM. The graphs are obtained through the above comparison techniques.

Simulation parameters consist of network simulator environmental attributes, which are used to establish the NS-2 implementation process. Simulation parameters describe rates and values of parameters, which are used in the F3TM Framework. Table 1 includes Channel, Mac Layer, Max Packet, Mobility Model, Number of Attackers, Number of Nodes, Propagation, Propagation Model, Queue, Radio Range, Routing Protocol, Simulation Time, Traffic Source, the X dimension of the topography, and the Y dimension of the topography.

The initialization and past interaction history factors are tabulated based on the above simulation, and the past interaction history of the concern. Here the iteration on the same path calculation is based on Eq. (7), and the route on the gateway is based on Eq. (8).

Table 2 consists of a network node explanation with regard to the network ID, next hop, current gateway node, cost,

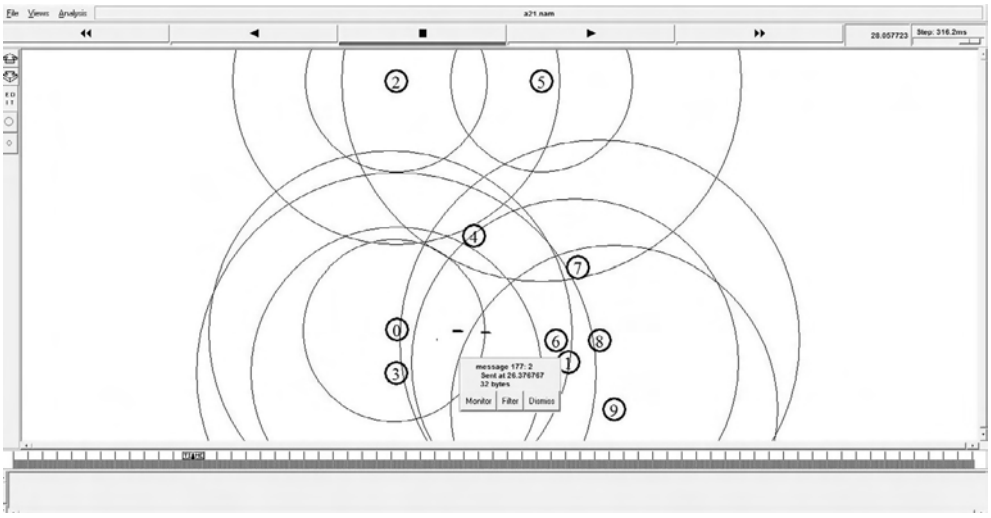

Figure 5 Simulation model of the network.

Table 1 Simulation parameters.

Simulation parameter	Value
Antenna	Omni antenna
Channel	Wireless channel
Mac layer	802.11
Max packet	100
Mobility model	Random way point
Number of attackers	5, 10, 15, 20, 25, 30
Number of nodes	50, 100, 150, 200
Propagation	Two ray ground
Propagation model	Two ray ground
Queue	Droptail/PriQueue
Radio range	250 M
Routing protocol	F3TM
Simulation time	200 s
Traffic source	CBR (constant bit rate)
The X dimension of the topography	1000
The Y dimension of the topography	1000

number of iterations and number of routes on the gateway, used for the past interaction history of the particular node.

Table 3 consists of the network node analysis of the interaction history values of nodes, in terms of network ID, next hop, current gateway node, cost, the number of iterations and the number of routes on the gateway, the values of which are tabulated by the system generated simulation parameters in Table 1. The node patterns were described based on the outer boundary values, which have been classified and named as trusted and untrusted parameters.

Trusted patterns enable the region boundary mobile nodes and untrusted patterns described, as based on the outer boundary region, both of which are listed based on the node location on MANET. The trust values for both the sender and receiver have been calculated through the use of Eq. (6). Likewise, the lifetime of the node, and its bandwidth and efficiency were illustrated in the experimental simulation, through the use of the network simulation tool-2. Finally, the past interaction history of the process is useful for verifying and reusing the past network process.

8.2. Evaluation metrics

The performance metrics of this work have been measured through the following criteria, including packet delivery ratio, overhead, delay and throughput. All those parameters show efficient results toward the F3TM framework, when compared with the AODV and DSDV. These results are discussed below in Table 4, and all evaluation criteria are measured based on the attacker presence in the network, as well as the number of nodes delivered to the destination with respect to the TFA.

Table 4 consists of the consolidated parameters of the node, including the number of hops, the sequence number of the concerned node, the time taken for the installation, and the time

Table 2 General past interaction history.

Network ID		Next hop	Current node to gateway	Cost	No. of nodes presented	No. of iterations of same path	No. of routes on the gateway
Network destination	Net mask	Gateway	Interface	Metric			
0.0.0.0	0.0.0.0	192.168.0.1	192.168.0.100	10	126	1260	2
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1	16,382	16,382	7
192.168.0.0	255.255.255.0	192.168.0.100	127.0.0.1	10	100	1000	1
192.168.0.100	255.255.255.255	127.0.0.1	127.0.0.1	10	27,889	278,890	11
192.168.0.1	255.255.255.255	192.168.0.100	192.168.0.100	10	27,734	277,340	11

Table 3 Past interaction history analysis values.

Network ID		Node pattern	Trust value		Lifetime (Ms)	Efficiency	Bandwidth
Network destination	Net mask		Sender node	Receiver node			
0.0.0.0	0.0.0.0	Untrusted	4	96	0.3	96	High
127.0.0.0	255.0.0.0	Trusted	2	98	0.2	93	Low
192.168.0.0	255.255.255.0	Trusted	20	90	0.01	94	Low
192.168.0.100	255.255.255.255	Untrusted	10	90	0.11	94	High

interval received packet count. All the above parameters are used to calculate the delay, control overhead, packet delivery ratio and throughput.

8.2.1. Average delay

Average delay is calculated by taking the delays for every data packet transmitted to the total number of received packets, as defined below in Eq. (9). With respect to the received control packets, the sent data packet is measured with the node properties. Based on the delay parameter of the individual node capabilities, the packet delay was measured and tabulated in Table 5.

$$\text{Average Delay} = \frac{\text{Sum of All Packets Delay}}{\text{Total No of Received Packets}} \tag{9}$$

Table 5 consists of the private IP address-based node, which has been sent through the network path. Each path has some transmission medium, such as a gateway IP address. This is used to direct the packet direction and the node properties, and it is significant for measuring the packet delay between the nodes.

Similarly, all other packet transmission delays are calculated based on Eq. (9), and there is a comparison of both the PRIME and CORMAN techniques, with the proposed F3TM, with respect to the AODV protocol. The average delay for selecting the paths is graphed below.

Fig. 6 shows the graph of the average delay taken for F3TM and PRIME and CORMAN with AODV. Both the PRIME and CORMAN have high average delays, comparable with F3TM and AODV.

8.2.2. Overhead

The packet overhead refers to the time taken to transmit data on a network. Each packet requires extra bytes of data, and a control packet added to the transmitted data, in order to carry out the routing information and the error correcting and operational instructions of the particular data. The energy consumption or packet lost during delivery from the source to the destination, which will reduce the overall transmission speed of the raw data, defines the ratio of the total number of control packets generated to the total number of data packets received, during the simulation time.

$$\text{Overhead} = \frac{\text{Data packets received}}{\text{Control packets generated}} \tag{10}$$

Generally, the received data packets and the received control packets are helpful for finding the overhead, with respect to the attacker node presence. Here three frameworks are compared, namely PRIME, CORMAN and F3TM, with the presence of attackers in the network with AODV (see Table 6).

Fig. 7 shows the overhead graph for CORMAN and PRIME Overhead and F3TM. It shows that PRIME and CORMAN have high Overhead values, whereas the proposed F3TM with AODV takes lesser values (see Table 7).

8.2.3. Packet delivery ratio (PDR)

The packet delivery ratio is the ratio between the numbers of packets successfully received at the destinations, and the total number of packets sent by sources defined in Eq. (11). The number of data packets delivered to the destination illustrates the level of data delivered to the destination. Mathematically, the information can be defined as follows:

$$\text{Packet delivery ratio} = \frac{\text{Received packets}}{\text{Sent packets}} * 100 \tag{11}$$

The following Fig. 8 shows the fractions of data packets, which are successfully delivered during the simulation time, versus the number of nodes in the presence of an attacker's interruption of the transmission nodes. Performance of the F3TM reduces regularly, while the packet delivery ratio increases in the case of F3TM and AODV. Finally, experimental results have shown that F3TM is better among the AODV protocols CORMAN and PRIME, with even the AODV protocol having the attacker in the MANET.

Fig. 8 shows the graph of PDR for CORMAN, and the PRIME frameworks which take the low PDR, and the proposed F3TM which takes the higher packet delivery ratio.

8.2.4. Throughput

On a technical level, throughput is described as the total number of packets successfully delivered per unit of time. The time window is the period during which the throughput is measured. The throughput is defined as the number of tasks completed in a given time period.

$$\text{Throughput} = \frac{\text{Total number of packets delivered successfully}}{\text{Total time internal}} \tag{12}$$

Table 8 presents the packet's delivery to the destination, and the calculation of the consolidated time interval for each node, which is useful for minimizing the throughput of the individual node transmission. This will become higher within the range of the particular node of the attacker presence. This has been illustrated in the following Fig. 9.

F3TM was evaluated for a period of time, with the proposed algorithms helping to offer the best performance. Fig. 9 gives a throughput comparison of the existing techniques of CORMAN and PRIME frameworks, with the proposed F3TM within the AODV framework. From this, it is

Table 4 Consolidated parameters of performance analysis.

Next hop (neighbor node)	Number of hops	Sequence number	Installation time (Ms)	Time interval (Ms)	Packets received		Over head	Average delay	Sent packets	Packet loss	PDR	Time interval
					Data packet	Control packet						
192.168.0.1	0	A46	001000	0.001	300	100	3	0.05	8500	500	94.25	0.7661
127.0.0.1	1	B36	001200	0.002	400	100	4	1	450	50	91.00	0.8611
192.168.0.100	2	C28	001500	0.005	600	100	6	7	350	50	87.75	1.0952
127.0.0.1	3	D11	001700	0.008	800	100	8	4	250	25	85.75	1.1111
192.169.0.100	4	E9	001600	0.007	1000	100	10	7.5	175	30	83.04	1.2055
192.169.0.100	5	F2	001900	0.005	1100	100	13	10	150	20	81.00	1.2600

Table 5 Calculation of the average delay.

Total number of packets		Received packets	Packet delay (with respect to the attackers)		
Received control packets	Received data packets		PRIME with AODV	CORMAN with AODV	F3TM with AODV
100	300	8000	4	6	0
100	400	500	6	8	1
100	600	300	8	12	7
100	800	225	14	17	4
100	1000	145	20	22	8
100	1100	130	22	23	10

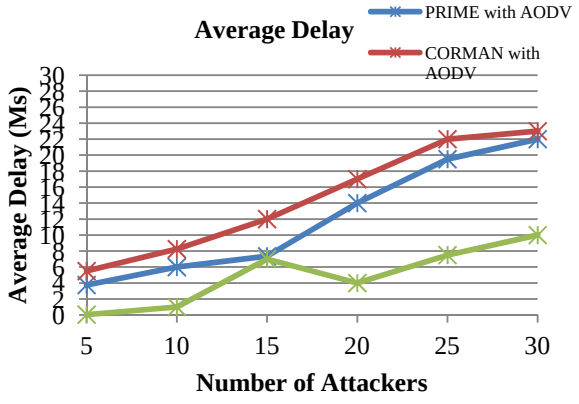

Figure 6 Comparison graph of the average delay of F3TM with AODV, and CORMAN and PRIME with AODV.

Table 6 Calculation of control overhead.

The total number of packets		Overhead		
Received control packets	Received data packets	PRIME with AODV	CORMAN with AODV	F3TM with AODV
100	300	5	9	3
100	400	7	11	4
100	600	9	14	6
100	800	12	16	8
100	1000	14	18	10
100	1100	16	20	13

clearly shown that the proposed technique achieves a better throughput than the existing technique.

Finally, the resultant quality of factors, like delay, packet delivery ratio, throughput, and overhear for various frameworks like PRIME and CORMAN, were compared with the F3TM framework. The PRIME framework is based on interest-defined mesh enclaves, with efforts that archive similar or better data delivery and end-to-end delays, and that approach is used for routing. The CORMAN framework is Cooperative Opportunistic Routing in mobile ad hoc networks, used for the path selection aspect using the lightweight proactive source routing protocol. In addition to that, all the frameworks are applied to the AODV routing protocol, and offer a comparison to those in the path selection. The one that will achieve the F3TM is a better Framework, when compared to all others. Those results prove that the Flooding Factor

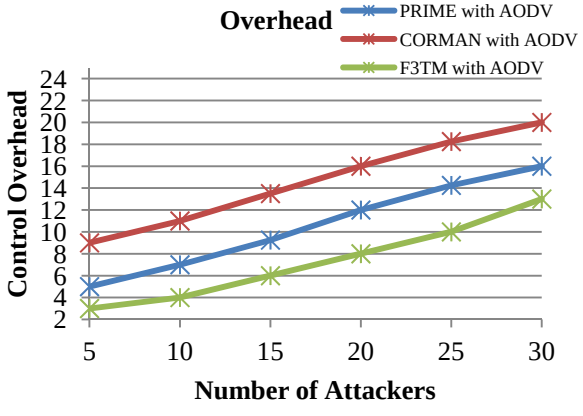

Figure 7 Comparison graph of the overhead of F3TM with AODV, and CORMAN and PRIME with AODV.

Table 7 Calculation for packet delivery ratio.

Number of packets received	Number of packets sent over the network	Packets lost	Packet delivery ratio		
			PRIME with AODV	CORMAN with AODV	F3TM with AODV
8000	8500	500	92	89	94
500	450	50	89	86	91
300	350	50	86	82	88
225	250	25	83	88	86
145	175	30	80	78	83
130	150	20	78	75	81

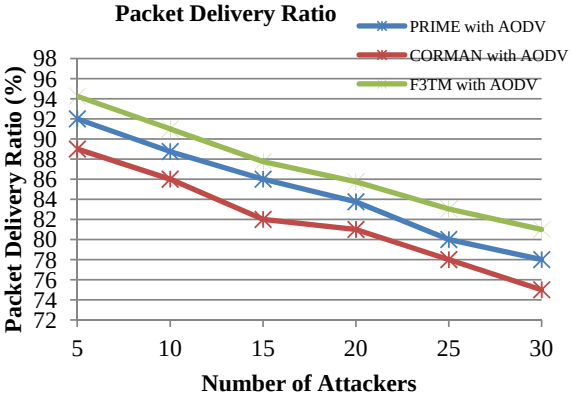

Figure 8 Comparison graph of the PDR of F3TM with AODV, and CORMAN and PRIME with AODV.

Table 8 Calculation of throughput.

Total number Of packets received	Consolidated time interval for each node (Ms)	Throughput		
		PRIME with AODV	CORMAN with AODV	F3TM with AODV
300	0.7661	13	9	15
400	0.8611	14	11	16
600	1.0952	12	7	18
800	1.1111	12	14	20
1000	1.2055	12	20	23
1100	1.2600	13	22	25

based Trust Management Framework (F3TM) for the mobile ad hoc network is secure in MANET. Each and every process makes the F3TM efficient for data transmission.

9. Conclusion

In this paper, a Flooding Factor based Framework for Trust Management (F3TM) has been presented using calculated trust value as the identification for malicious nodes. From the design, development and evaluation of the proposed framework, following conclusions have been made. F3TM is useful

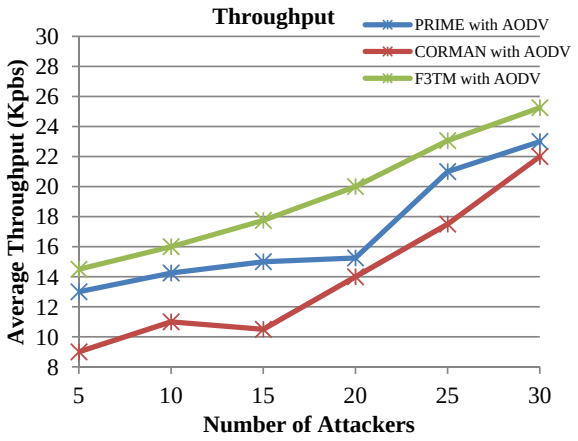

Figure 9 Comparison graph of the throughput of F3TM with AODV, and CORMAN and PRIME with AODV.

for secure data dissemination in scalable MANET environment. Experimental Grey Wolf algorithm based node validation and Multi-Swarm Optimization based route selection is beneficial for optimal and efficient data dissemination. Average packet delivery delay of F3TM is lower as compared to that of PRIME and CORMAN. F3TM generates lesser control overheads in comparison with the state-of-the-art techniques. Packet delivery ratio and throughput of F3TM are significantly higher than those of the state-of-the-art techniques.

References

Al Mazrouei, M.S., Narayanaswami, S., 2011. Mobile ad hoc networks: a simulation based security evaluation and intrusion prevention. In: Internet Technology and Secured Transactions (ICITST), 2011 International Conference for, pp. 308–313.

Assis, K.D.R., Giozza, W.F., 2010. Hybrid algorithms for routing and assignment wavelengths in optical networks. Lat. Am. Trans. IEEE (Revista IEEE Am. Lat.) 8 (3), 214–220.

Bindra, G.S., Kapoor, A., Narang, A., Agrawal, A., 2012. Detection and removal of co-operative blackhole and grayhole attacks in MANETs. In: System Engineering and Technology (ICSET), 2012 International Conference on, pp. 1–5.

Chang, B.-J., Kuo, S.-L., Liang, Y.-H., Wang, D.-Y., 2008. Markov chain-based trust model for analyzing trust value in distributed multicasting mobile ad hoc networks. In: Asia-Pacific Services Computing Conference, 2008. APSCC'08. IEEE, pp. 156–161.

Dahiya, P., Johari, R., 2014. VAST: volume adaptive searching technique for optimized routing in mobile ad-hoc networks. In: Advance Computing Conference (IACC), 2014 IEEE International, pp. 1–6.

Garcia-Luna-Aceves, J.J., Menchaca-Mendez, R., 2011. PRIME: an interest-driven approach to integrated unicast and multicast routing in MANETs. Networking IEEE/ACM Trans. 19 (6), 1573–1586.

Gorlatova, M., Mason, P.C., Wang, M., Lamont, L., Liscano, R., 2006. Detecting wormhole attacks in mobile ad hoc networks through protocol breaking and packet timing analysis. In: Military Communications Conference, 2006. MILCOM 2006. IEEE, pp. 1–7.

Guo, J., Marshall, A., Zhou, B., 2011. A new trust management framework for detecting malicious and selfish behaviour for mobile ad hoc networks. In: Trust, Security and Privacy in Computing and

Communications (TrustCom), 2011 IEEE 10th International Conference on, pp. 142–149.
Jain, S.A., Raisinghani, V.T., 2014. Load equilibrium neighbor aware routing in mobile ad hoc network. In: India Conference (INDICON), 2014 Annual IEEE, pp. 1–6.
Jaiswal, R., Sharma, S., 2012. Relative cluster entropy based wormhole detection using AOMDV in ad hoc network. In: Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on, pp. 747–752.
Lacharité, Y., Nguyen, D.Q., Wang, M., Lamont, L., 2008. A trust-based security architecture for tactical MANETS. In: Military Communications Conference, 2008. MILCOM 2008. IEEE, pp. 1–7.
Lafta, H.A., Al-Salih, A.M.M.S., 2014. Efficient routing protocol in the mobile ad-hoc network (MANET) by using genetic algorithm (GA). IOSR J. Comput. Eng. 16 (1), 47–54.
Long, Y., Li, H., Pan, M., Fang, Y., Wong, T.F., 2013. A fair QoS-aware resource-allocation scheme for multiradio multichannel networks. Veh. Technol. IEEE Trans. 62 (7), 3349–3358.
Manikandan, K.P., Satyaprasad, D.R., Rajasekhararao, D.K., 2011. A survey on attacks and defense metrics of routing mechanism in mobile ad hoc networks. IJACSA Int. J. Adv. Comput. Sci. Appl. 2 (3).
McNerney, P.J.J., Zhang, N., 2012. A study on reservation-based adaptation for QoS in adversarial MANET environments. In: Wireless Communications and Mobile Computing Conference (IWCMC), 2012 8th International, pp. 677–682.
Perkins, C.E., Bhagwat, P., 1994. Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. ACM SIGCOMM Comput. Commun. Rev. 24 (4), 234–244.
Qureshi, B., Min, G., Kouvatsos, D., 2010. Collusion detection and prevention with fire+ trust and reputation model. In: Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on, pp. 2548–2555.
Rmayti, M., Begriche, Y., Khatoun, R., Khoukhi, L., Gaiti, D., 2014a. Denial of service (DoS) attacks detection in MANETs using Bayesian classifiers. In: Communications and Vehicular Technology in the Benelux (SCVT), 2014 IEEE 21st Symposium on, pp. 7–12.
Rmayti, M., Begriche, Y., Khatoun, R., Khoukhi, L., Gaiti, D., 2014b. Denial of Service (DoS) attacks detection in MANETs through statistical models. In: Global Information Infrastructure and Networking Symposium (GIIS), pp. 1–3.
Vadivel, R., Narasimhan, B., 2014. A reliable flooding mechanism for mobile ad-hoc networks. In: Intelligent Computing Applications (ICICA), 2014 International Conference on, pp. 301–304.
Wang, Z., Chen, Y., Li, C., 2012. CORMAN: a novel cooperative opportunistic routing scheme in mobile ad hoc networks. Sel. Areas Commun. IEEE J. 30 (2), 289–296.
Wei, Z., Tang, H., Yu, F.R., Wang, M., Mason, P., 2014. Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning. Veh. Technol. IEEE Trans. 63 (9), 4647–4658.
Yang, B., Yamamoto, R., Tanaka, Y., 2014. Dempster-Shafer evidence theory based trust management strategy against cooperative black hole attacks and gray hole attacks in MANETs. In: Advanced Communication Technology (ICACT), 2014 16th International Conference on, pp. 223–232.